REMARKS

I. Introduction

Claims 1 – 21 are currently pending. In response to the Office Action dated June 4, 2008, please consider the following remarks. Re-examination and re-consideration of the application, is requested.

II. Double Patenting Rejection

In paragraph 2, the Office Action provisionally rejects claim(s) 1-21 under the judicially-created doctrine of double patenting as being unpatentable over:

- The pending claims of co-pending application serial number 09/620,772
- The pending claims of co-pending application serial number 09/620,833
- The pending claims of co-pending application serial number 10/758,865
- The pending claims of co-pending application serial number 10/758,818

The Applicant respectfully traverses, because the claims of the instant application cannot be said to be obvious over the claims of the cited co-pending applications. Claim 1 of the instant application is instructive. It recites the use of a family pairing key and use of that key to generate copy protection keys for client receivers:

> *A method of distributing video content from a broadcast system between a host receiver and a client receiver, comprising:*
> *(a) transmitting a family pairing key from the broadcast system to both the host receiver and the client receiver;*
> *(b) decrypting program materials received by the host receiver from the broadcast system;*
> *(c) generating a copy protection key at the host receiver using the family pairing key;*
> *(d) encrypting the decrypted program materials at the host receiver using the copy protection key;*
> *(e) transferring the encrypted program materials from the host receiver to the client receiver;*
> *(f) generating the copy protection key at the client receiver using the family pairing key; and*
> *(g) decrypting the transferred program materials at the client receiver using the copy protection key.*

The issue is whether any of the *claims* of the above-cited applications are obvious variations of the *claims* of the pending applications. For the reasons below, the Applicants respectfully submit the claims of the instant case are not obvious over the claims of any of the claims of the co-pending cases.

A. With Respect to Co-Pending Application Serial Number 09/620,772

The first independent claim of the '772 application is shown below:

1. (PREVIOUSLY PRESENTED) A method of storing program material in a media storage device communicatively coupled to a receiver for subsequent replay, comprising the steps of:

(a) accepting encrypted access control information and the program material encrypted according to a first encryption key in the receiver, the access control information including a first encryption key and control data;

(b) decrypting the received access control information in a conditional access module releasably coupleable with the receiver to produce the first encryption key;

(c) decrypting the program material in the receiver using the first encryption key;

(d) re-encrypting the program material according to a second encryption key;

(e) encrypting the second encryption key in the conditional access module according to a third encryption key to produce a fourth encryption key; and

(f) providing the re-encrypted program material and the fourth encryption key for storage external to the conditional access module.

Plainly, this claim discloses nothing about the use of a family key. The other pending claims likewise make no mention of a family key used in the way specified in claim 1. Accordingly, with respect to this application, the double patenting rejection is improper and should be withdrawn.

B. With Respect to Co-Pending Application Serial Number 09/620,833

The first independent claim of the '833 patent application is shown below:

1. (CURRENTLY AMENDED) A method of storing program material for subsequent replay, comprising the steps of:

receiving a data stream comprising program material encrypted according to a first encryption key;

decrypting the program material;

re-encrypting the decrypted program material according to a receiver-unique second encryption key and encrypting the receiver-unique second encryption key according to a receiver-unique third encryption key to produce a fourth encryption key;

storing the re-encrypted program material in a media storage device;

storing the fourth encryption key;

retrieving the stored re-encrypted program material; and

decrypting the retrieved re-encrypted program material[;].

~~wherein the step of re-encrypting the decrypted program material according to a second encryption key comprises the steps of re-encrypting the decrypted program material according to the second encryption key, and encrypting the second key according to a receiver-unique third key to produce a fourth encryption key.~~

There is no mention of the use of a family key. Further, the remaining claims of the '833 patent do not recite a family key. Accordingly, with respect to this application, the double patenting rejection should be withdrawn.

C. With Respect to Co-Pending Application Serial Number 10/758,865

The first independent claim of the '865 patent application recites:

1. (CURRENTLY AMENDED) A method of operatively pairing a host receiver and a client receiver in a broadcast system, comprising:

(a) receiving encrypted program materials, generated by a service provider, at one or more subscriber receiving stations, at least one of the subscriber receiving stations being comprised of a plurality of networked receivers, wherein the networked receivers include at least one host receiver and at least one client receiver;

(b) decrypting the received program materials at the host receiver;

(c) re-encrypting the decrypted program materials at the host receiver using a copy protection key;

(d) encrypting the copy protection key at the host receiver using a host-client pairing key generated by the service provider and shared between the host receiver and client receiver in order to share the program materials between the host receiver and client receiver, wherein the service provider establishes the host-client pairing key for a particular combination of the host and client receivers;

(e) transferring the re-encrypted program materials and the encrypted copy protection key from the host receiver to the client receiver;

(f) decrypting the transferred copy protection key at the client receiver using the host-client pairing key; and

(g) decrypting the transferred program materials at the client receiver using the decrypted copy protection key.

As a threshold matter, the Applicants have already filed a terminal disclaimer with respect to the '865 application. However, as discussed below, the Applicants are petitioning to withdraw the '865 terminal disclaimer because it was not necessary and improvidently filed.

The instant case recites the use of a family pairing key that is transmitted to the host and *used to generate a copy protection key that is then shared between the host and the client.* The claims of the '865 patent, however, recite a host-client pairing key that is generated by the service provider and shared between the host receiver and the client receiver. There is no notion of generating the copy protection key in the host from the pairing key. Therefore, even if the host-client pairing key were analogous to the family pairing key, it is generated differently and used differently. Accordingly, the instant application's claims are not obvious compared to the '865 patent claims.

Finally, MPEP § 804 (I)(B)(1) states:

> If a "provisional" nonstatutory obviousness-type double patenting (ODP) rejection is the only rejection remaining in the earlier filed of the two pending applications, while the later-filed application is rejectable on other grounds, the examiner should withdraw that rejection and permit the earlier-filed application to issue as a patent without a terminal disclaimer. If the ODP rejection is the only rejection remaining in the later-filed application, while the earlier-filed application is rejectable on other grounds, a terminal disclaimer must be required in the later-filed application before the rejection can be withdrawn.

In the instant case, assuming the terminal disclaimer and double patenting rejection relating to issued patent 7,203,314 are withdrawn, the nonstatutory obviousness-type double patenting rejection based on 10/758,865 is one of a number of nonstatutory obviousness type double patenting rejections that are the only rejections remaining in this pending application. Further, application serial number 10/758,865 remains rejected on other grounds. The double patenting rejection of the instant case over the claims of 10/758,865 should be withdrawn for this reason as well.

The Applicants have also petitioned that the terminal disclaimer already filed with respect to the '865 application be withdrawn.

D. With Respect to Co-Pending Application Serial Number 10/758,818

The first independent claim of the '818 application is shown below:

1. (PREVIOUSLY PRESENTED) A method of distributing program materials received from a broadcast system between a host receiver and a client receiver for remote decryption, comprising:

(a) receiving an encrypted media encryption key at the host receiver;

(b) decrypting the encrypted media encryption key at the host receiver;

(c) re-encrypting the decrypted media encryption key at the host receiver using a pairing key;

(d) transferring the re-encrypted media encryption key from the host receiver to the client receiver, wherein the client receiver does not utilize a conditional access module (CAM);

(e) decrypting the re-encrypted media encryption key at the client receiver using the pairing key;

(f) receiving encrypted program materials from the broadcast system at the host receiver;

(g) transferring the encrypted program materials from the host receiver to the client receiver; and

(h) decrypting the encrypted program materials at the client receiver using the decrypted media encryption key.

Again, the foregoing claim does not recite generating a copy protection key at the host key using a family pairing key or generating a copy protection key at the client using the family pairing key. Likewise, none of the remaining claim appear to disclose this feature. Accordingly, this double patenting rejection should be withdrawn.

E. Should the Examiner Maintain the Double Patenting Rejection(s)

The Office Action did not indicate which claims of the instant application are obvious in view of which claims of the applications referenced above, nor was a rationale provided. Should the Examiner decide to maintain any of the double patenting rejections, the Applicants respectfully request that some detail be provided indicating the basis for the rejection.

III. The Applicants Petition to Withdraw the Terminal Disclaimers Filed March 4, 2008

Included herewith is a Petition under 37 C.F.R. § 1.181 requesting withdrawal of the terminal disclaimers of 10/758,865 and U.S. Patent No. 7,203,314. The Examiner should be aware that the

Applicants are requesting that the these terminal disclaimers be withdrawn in light of the arguments presented below:

A. The Claims of the Instant Application are not Obvious in View of the Claims of U.S. Patent Application Serial No. 10/758,865

The impropriety of the double patenting rejection of the instant claims when compared to those of the '865 patent is discussed above. For the reasons cited, the Applicant respectfully petitions that the terminal disclaimer be withdrawn.

B. The Claims of the Instant Application are not Obvious in View of the Claims of U.S. Patent 7,203,314

The claims of U.S. Patent No. 7,203,314 are reproduced below:

1. A method of storing program material for subsequent replay, comprising the steps of:
receiving encrypted access control information and the program material encrypted according to a first encryption key, the encrypted access control information including a first encryption key and temporally-variant control data;
decrypting the encrypted access control information to produce the temporally-variant control data;
modifying the temporally-variant control data to generate temporally-invariant control data;
re-encrypting the access control information including the temporally-invariant control data;
further encrypting the encrypted program material according to a second encryption key;
encrypting the second encryption key according to a third encryption key to produce a fourth encryption key;
and storing the further encrypted program material and the encrypted access control information and the fourth encryption key.

2. The method of claim 1, wherein
the temporally-variant control data associates an expiration time with the program material and wherein: the step of modifying the temporally variant control data to generate temporally-invariant control data further comprises the steps of decrypting the received access control information to produce the first encryption key and the temporally-variant control data, and modifying the expiration time associated with the program material;
and the step of re-encrypting the access control information comprises the step of re-encrypting the first encryption key and the temporally-invariant control data.

3. The method of claim 1, wherein the step of re-encrypting the access control information comprises the step of encrypting the access control information including the temporally-invariant control data and the first encryption key according to a fifth encryption key.

4. The method of claim 1, wherein: the step of modifying the temporally-variant control data to generate temporally invariant control data is performed by a smartcard.

5. The method of claim 1, further comprising the steps of:
retrieving the stored further encrypted program material, the encrypted access control information, and the encrypted fourth encryption key;
decrypting the encrypted fourth encryption key to produce the second encryption key using the third

encryption key;
decrypting the further encrypted program material using the second encryption key;
decrypting the access control information to produce the first encryption key;
and decrypting the encrypted program material using the first encryption key.

6. The method of claim 5, wherein the step of decrypting the access control information to produce the first encryption key is performed in response to receiving a pay-per-view (PPV) request from the user.

7. The method of claim 5, further comprising the steps of:
further encrypting the encrypted access control information according to the second encryption key before storing the encrypted access control information;
and decrypting the further encrypted access control information according to the second encryption key to produce the encrypted temporally-invariant control data before decrypting the access control information.

8. The method of claim 7, wherein the step of decrypting the first encryption key is performed in response to receiving a pay-per-view request from the user.

9. The method of claim 1, wherein the steps of modifying the temporally-variant control data to generate temporally-invariant control data and re-encrypting the access control information including the temporally-invariant control data is performed in response to a pre-buy message.

10. The method of claim 1, wherein the access control information further comprises metadata describing viewing rights for the program material.

11. The method of claim 10, further comprising the step of: generating the second encryption key from information including the metadata.

12. The method of claim 10, wherein the step of re-encrypting the access control information comprises the step of encrypting the access control information including the temporally-invariant control data and the first encryption key according to a fourth encryption key, and the method further comprises the step of: generating the fourth encryption key from information including the metadata.

13. A method of storing program material for subsequent replay, comprising the steps of:
receiving access control information and the program material encrypted according to a first encryption key, the access control information including a first encryption key and temporally-variant control data;
further encrypting the encrypted program material and temporally-variant control data according to a second encryption key;
encrypting the second encryption key according to a third encryption key to produce a fourth encryption key;
and storing the further encrypted program material and the temporally-variant control data and the fourth encryption key.

14. The method of claim 13, wherein the temporally-variant control data associates broadcast channel and expiration time with the program material.

15. The method of claim 13, further comprising the steps of:
reading the stored further encrypted program material and the temporally-variant data and the fourth encryption key;
decrypting the fourth encryption key using the fourth encryption key to produce the second encryption key;
decrypting the further encrypted program material using the second encryption key;
decrypting the first encryption key using the fourth encryption key;
and decrypting the encrypted program material using the first encryption key.

16. An apparatus for storing program material for subsequent replay, comprising:

a conditional access module, for accepting encrypted access control information and the program material encrypted according to a first encryption key, the encrypted access control information including the first encryption key and temporally-variant control data, the conditional access module having a first decryptor module, for decrypting the encrypted access control information to produce the temporally variant control data;

a conversion module for modifying the temporally-variant control data to produce temporally-invariant control data;

a re-encryptor module, for re-encrypting the decrypted access control information;

a second decryptor module for decrypting the re-encrypted access control information to produce the first encryption key;

a copy protection encryption module, communicatively coupleable to the conditional access module and a media storage device, the copy protection encryption module for further encrypting the encrypted program material according to a second encryption key and for encrypting the second encryption key according to a third encryption key to produce a fourth encryption key;

and a copy protection decryption module, communicatively coupleable to the conditional access module and the media storage device, the copy protection decryption module for decrypting the encrypted fourth encryption key to produce the second encryption key using the third encryption key.

17. The apparatus of claim 16, further comprising: a tuner, communicatively coupleable to the conditional access module, for receiving the encrypted access control information and the program material encrypted according to a first encryption key, the encrypted access control information including a first encryption key and temporally-variant control data.

18. The apparatus of claim 16, further comprising the media storage device.

19. The apparatus of claim 16, wherein:

the copy protection encryption module further encrypts re-encrypted access control information according to the second encryption key;

and the copy protection decryption module further decrypts the further encrypted re-encrypted access control information according to the second encryption key.

20. The apparatus of claim 16, wherein the temporally-variant control data associates an expiration time with the program material, and the conversion module modifies the expiration time associated with the program material.

21. The apparatus of claim 16, wherein the access control information further comprises metadata describing viewing rights for the program material and wherein the re-encryptor module re-encrypts the decrypted access control information according to a fifth encryption key generated at least in part from the metadata.

22. The apparatus of claim 16, wherein the access control information further comprises metadata describing viewing rights for the program material and the second encryption key is generated at least in part from the metadata.

23. The apparatus of claim 16, wherein the conditional access module is implemented in a smartcard.

24. The apparatus of claim 16, wherein the smartcard is releaseably communicatively coupleable with the tuner.

25. An apparatus for storing program material for subsequent replay, comprising:

means for receiving encrypted access control information and the program material encrypted according to a first encryption key, the encrypted access control information including a first encryption key and temporally-variant control data;

means for decrypting the encrypted access control information to produce the temporally-variant control data;

means for modifying the temporally-variant control data to generate temporally-invariant control data;

means for re-encrypting the access control information including the temporally-invariant control data;

means for further encrypting the encrypted program material according to a second encryption key;

means for encrypting the second encryption key according to a third encryption key to produce a fourth encryption key;

and means for storing the further encrypted program material and the encrypted access control information and the fourth encryption key.

26. The apparatus of claim 25, wherein the temporally-variant control data associates an expiration time with the program material and wherein:

the means for modifying the temporally variant control data to generate temporally-invariant control data further comprises means for decrypting the received access control information to produce the first encryption key and the temporally-variant control data, and means for modifying the expiration time associated with the program material;

and the means for re-encrypting the access control information comprises the step of re-encrypting the first encryption key and the temporally-invariant control data.

27. The apparatus of claim 25, wherein the means for re-encrypting the access control information comprises means for encrypting the access control information including the temporally-invariant control data and the first encryption key according to a fourth encryption key.

28. The apparatus of claim 25, wherein: the means for modifying the temporally-variant control data to generate temporally invariant control data is performed by a smartcard.

29. The apparatus of claim 25, further comprising:

means for retrieving the stored further encrypted program material, the encrypted access control information, and the encrypted fourth encryption key;

means for decrypting the encrypted fourth encryption key to produce the second encryption key using the third encryption key;

means for decrypting the further encrypted program material using the second encryption key;

means for decrypting the access control information to produce the first encryption key;

and means for decrypting the encrypted program material using the first encryption key.

30. The apparatus of claim 29, wherein the decryption of the access control information to produce the first encryption key is performed in response to receiving a pay-per-view (PPV) request from the user.

31. The apparatus of claim 29, further comprising:

means for further encrypting the encrypted access control information according to the second encryption key before storing the encrypted access control information;

and means for decrypting the further encrypted access control information according to the second encryption key to produce the encrypted temporally-invariant control data before decrypting the access control information.

32. The apparatus of claim 29, wherein the means for decrypting the first encryption key is performed in response to receiving a pay-per-view request from the user.

33. The apparatus of claim 25, wherein the means for modifying the temporally-variant control data to generate temporally-invariant control data and re-encrypting the access control information including the temporally-invariant control data is performed in response to a pre-buy message.

34. The apparatus of claim 25, wherein the access control information further comprises metadata

describing viewing rights for the program material.

35. The apparatus of claim 34, further comprising: means for generating the second encryption key from information including the metadata.

36. The apparatus of claim 34, wherein the means for re-encrypting the access control information comprises means for encrypting the access control information including the temporally-invariant control data and the first encryption key according to a fourth encryption key, and the apparatus further comprises: means for generating the fourth encryption key from information including the metadata.

37. An apparatus for storing program material for subsequent replay, comprising:
means for receiving access control information and the program material encrypted according to a first encryption key, the access control information including a first encryption key and temporally-variant control data;
means for further encrypting the encrypted program material and temporally-variant control data according to a second encryption key;
means for encrypting the second encryption key according to a third encryption key to produce a fourth encryption key;
and means for storing the further encrypted program material and the temporally-variant control data and the fourth encryption key.

38. The apparatus of claim 37, wherein the temporally-variant control data associates broadcast channel and expiration time with the program material.

39. The apparatus of claim 37, further comprising:
means for reading the stored further encrypted program material and the temporally-variant data and the fourth encryption key;
means for decrypting the fourth encryption key using the fourth encryption key to produce the second encryption key;
means for decrypting the further encrypted program material using the second encryption key;
means for decrypting the first encryption key using the fourth encryption key;
and means for decrypting the encrypted program material using the first encryption key.

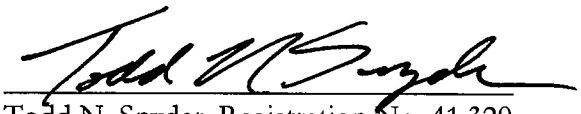
As can be seen by inspection, none of thee claims recites the use of a family key or anything analogous to it. Accordingly, the claims of the instant application are not obvious over the claims of 7,203,314.

IV. Conclusion

In view of the above, it is submitted that this application is now in good order for allowance and such allowance is respectfully solicited. Should the Examiner believe minor matters still remain that can be resolved in a telephone interview, the Examiner is urged to call Applicants' undersigned attorney.

Respectfully submitted,

Date: September 4, 2008



Todd N. Snyder, Registration No. 41,320
Attorney for Applicants

The DIRECTV Group, Inc.
CA / LA1 / A109
2230 E. Imperial Highway
El Segundo CA 90245

Telephone No. (310) 964-0560